Notice of Allowability	Application No.	Applicant(s)	
	10/527,368	AHONEN ET AL.	
	Examiner	Art Unit	
	Sarah Su	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *amendment filed 30 April 2009*.

2. ☒ The allowed claim(s) is/are *1-13 and 15-25*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *7/7/09* .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

/Sarah Su/
Examiner, Art Unit 2431

NOTICE OF ALLOWANCE

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 30 April 2009 has been entered. In this amendment, claims 1, 7, 11, 13, 16, 17, and 20 have been amended.

2. Claims 1-13 and 15-25 are presented for examination.

Response to Arguments

3. Applicant's arguments with respect to the objection to claims 4, 11, and 13 have been fully considered and are persuasive. The objection of 30 December 2008 has been withdrawn.

4. Applicant's arguments with respect to the rejection of claims 1-13 and 15-25 under 35 USC 103 have been fully considered and are persuasive. The rejection of 30 December 2008 has been withdrawn.

EXAMINER'S AMENDMENT

5. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided

by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Sidney Weatherford on 7 July 2009.

The application has been amended as follows:

In claim 1, line 8: delete "the registration message" and insert –the join request message–.

In claim 1, line 21: delete "the candidate subscriber" and insert –a candidate subscriber–.

In claim 1, line 22: delete "the certificate" and insert –a certificate–.

In claim 7, line 2: after "a secure IP multicast or broadcast", insert –by distributing security keys to the user using a key revocation based mechanism–.

In claim 7, line 3: delete "distributing security keys to users using a key revocation based mechanism".

In claim 7, after line 8, insert:

-- the user sending a join request message to a group controller, the join request message including the user's originating IPv6 address, a copy of the user's public key from the user's public-private key pair and triggering a verification wherein a digital signature is returned to the group controller, the digital signature generated by applying a cryptographic hashing function to the user's private key, from the user's public-private

key pair, a random number and time stamp, both received from the group controller; --.

In claim 13, line 11: delete "a digital signature using" and insert –a digital signature, the digital signature generated by applying a cryptographic hashing function to–.

In claim 13, line 12: after "candidate member's public-private key pair", insert –, a random number and time stamp, both received from the group controller–.

In claim 13, line 16: delete "wherein the verifying means".

In claim 20, line 2: after "a secure IP multicast or broadcast", insert –by distributing security keys to the user using a key revocation based mechanism–.

In claim 20, lines 3-4: delete "means for distributing security keys to the user using a key revocation based mechanism".

In claim 20, after line 4: insert:

-- means for receiving a join request message from the user, the join request message including the user's originating IPv6 address, a copy of the user's public key from the user's public-private key pair;

means for verifying a digital signature generated by applying a cryptographic hashing function to the user's private key, from the user's public-private key pair, a random number and time stamp, both received from the group controller; --.

In claim 20, lines 5-6: delete "a public-private key pair" and insert –the public-private key pair–.

Allowable Subject Matter

6. Claims 1-13, and 15-25 are allowed.

7. The following is an examiner's statement of reasons for allowance:

Claims 1 and 13 recite "the candidate member sending a join request message to the group controller, the join request message including the candidate member's originating IPv6 address, a copy of the candidate member's public key from the candidate member's public-private key pair and a digital signature, the digital signature generated by applying a cryptographic hashing function to the candidate member's private key, from the candidate member's public-private key pair, a random number and time stamp, both received from the group controller." This feature, in combination with the other limitations in the claims, is not anticipated by, nor made obvious over, the prior art of record.

Claim 7 recites "the user sending a join request message to a group controller, the join request message including the user's originating IPv6 address, a copy of the user's public key from the user's public-private key pair and triggering a verification wherein a digital signature is returned to the group controller, the digital signature generated by applying a cryptographic hashing function to the user's private key, from the user's public-private key pair, a random number and time stamp, both received from

the group controller." This feature, in combination with the other limitations in the claims, is not anticipated by, nor made obvious over, the prior art of record.

Claim 20 recites "means for receiving a join request message from the user, the join request message including the user's originating IPv6 address, a copy of the user's public key from the user's public-private key pair" and "means for verifying a digital signature generated by applying a cryptographic hashing function to the user's private key, from the user's public-private key pair, a random number and time stamp, both received from the group controller." These features, in combination with the other limitations in the claims, are not anticipated by, nor made obvious over, the prior art of record.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Balfanz et al. (US 2007/0204149 A1) discloses a system and method providing secured communication.

b. Hardjono (US Patent 7,360,084 B1) discloses a system and method for controlling access in a multicast communication network.

c. Kim (US 2005/0097316 A1) discloses a system and method for using a digital signature based on identification information of group members.

d. Peterka et al. (US 2002/0174366 A1) discloses a system and method for the enforcement of content rights and conditions for multimedia content in a multicasting system.

e. Srivastava et al. (US 2005/0044356 A1) discloses a system and method for distributing and updating private keys of multicast group managers using directory replication.

f. Yegin et al. (US Patent 7,286,671 B2) discloses a system and method for secure network access.

g. Yosef et al. (US 2005/0259682 A1) discloses a system and method for emulating an interactive connection in a broadcast system.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Sarah Su whose telephone number is (571) 270-3835. The examiner can normally be reached on Monday through Friday 7:30AM-5:00PM EST..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on (571) 272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Sarah Su/
Examiner, Art Unit 2431

/William R. Korzuch/
SPE, Art Unit 2431